REMARKS

Claims 21-31 remain in the application.

The Rejections:

In the Office Action dated March 24, 2009, the Examiner rejected Claims 21-31 under 35 U.C. 103(a) as being unpatentable over Allen, et al. (US 6,000,505) and further in view of Scheidt (US 7,111,173).

Applicants' Response:

The Examiner stated that Allen remains the primary art which does not disclose the generation of a virtual key and does not go into further details of steps f-i related to the generated virtual key.

According to the Examiner, Scheidt discloses as a convenience the password is distributed to users that will unlock user credentials [Scheidt - col.5, lines 22-40]. Scheidt discloses the credentials includes passwords, biometric data, encryption key, and signature which are all used for authentication of a user [Scheidt - col. 8, lines 6-60 and col. 10, line 55 - col. 11, lines 20]. Thus, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine Allen with Scheidt teaching the limitations of virtual key in steps e-i because to authenticate users when starting a session [Scheidt - col. 8, lines 6-60 and col. 10, line 55 – col. 11, lines 20]

Allen refers to an elevator system operable as emergency egress and evacuation during a fire incident. Upon detection of a fire incident in a building, a communication mechanism sends a detection signal and a status signal to a remote fire department (col. 6, lines 1-7).

Scheidt describes a cryptographic key management system CKM for use with large distributed networks. A user receives a "first-use" password to access credentials and then changes the password. (col. 5, lines 22-40) The user credentials must decrypted before use with a key derived from the user's id and password.

The Examiner identified the detection of a fire incident in Allen as the "at least one initiating event" and suggests that the generation of a "first-use" password by the Scheidt Credential Manager software (col. 9, lines 5-10) somehow be combined with the Allen monitoring and control of the building's status to generate a "virtual key" (col. 20, lines 2-5). As the Examiner admitted, Allen does not disclose generating a "virtual key". Allen does not provide any reason to generate a "first-use" password for the fire department, nor is there any portion of the Allen process of monitoring and control of the building's status for which the Scheidt "first-use" password could be substituted.

Furthermore, Applicant's claims recite the steps of

g. detecting use of the virtual key by the at least one person in the building;

h. checking the validity of the virtual key; and

i. initiating the procedure within the building if the validity check is positive wherein initiating the procedure consists of performing at least one of the steps of:

opening of at least one door of the building;

making at least one elevator available;

opening of at least one elevator door; and

release of any security barriers which may be present;

Scheidt uses the "first-use" password only to enable a user of the computer system to decrypt credentials before they can be used for the first time. Once the credentials have been decrypted, a new password must be provided for subsequent encryption and decryption. (col. 9, lines 4-9) Thus, the result of a positive validity check of the "first-use" password will not result in the performance of Applicant's step "i" and the combination of Allen and Scheidt as proposed by the Examiner does not render Applicant's claims obvious.

Applicant does not believe that there is any motivation to combine the Scheidt computer network security system with the Allen elevator control system. Allen shows an automatic building evacuation system with a control unit programmed to automatically define an evacuation zone and to drive elevator cars to evacuate building occupants (col. 6, lines 18-35). For the building evacuation, the physical presence of

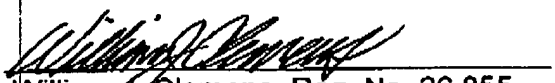
firemen is not necessary (col. 7, lines 22-24). The fire department can override the emergency evacuation from a building lobby or from a fire alarm panel (col. 8, lines 12-14). Access to the lobby or the panel occurs by using the ASME A17.1 code required fire department key (col. 4, lines 10-24).

Scheidt involves safeguarding data. Access to the data is restricted utilizing a combination of credentials and passwords to individually identify authorized users of the computer system. There is no reason to individually authenticate firemen prior to fighting a fire in a building. Therefore, neither Allen nor Scheidt generates a virtual key or transmits a virtual key to a person as recited in Applicant's Claims 21-31.

The Examiner listed prior art on Form PTO-892 without comment. The Examiner cited: Weinreich et al. (US 6175831), Faris et al. (US 6903681), Clarke (US 6920496), Sachs et al. (US 6331865), Backal (US 6219421), Peirce et al. (US 6157649) and Farry et al. (US 6069628). Applicant reviewed these references and found them to be no more pertinent than the prior art relied upon by the Examiner in the rejections.

In view of the above arguments, Applicant believes that the claims of record now define patentable subject matter over the art of record. Accordingly, an early Notice of Allowance is respectfully requested.

Respectfully submitted,



William J. Clemens, Reg. No. 26,855
(248) 960-2100

Fraser Clemens Martin & Miller LLC
28366 Kensington Lane
Perrysburg, Ohio 43551-4163
419-874-1100
419-874-1130 (FAX)